Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A secured and confidential method for transmitting a digital data file between a sending element and a receiving element via telecommunication or radiocommunication ~~networks,~~:networks, comprising:

- the sending element downloads ~~a database listing the authorized sending elements,~~ a symmetrical fragmentation-transmission secret ~~key~~ ;key from a database listing the authorized sending elements, wherein a size and content of the symmetrical fragmentation-transmission secret key is dependent on a size of the telecommunication or radiocommunication networks;

- the sending element transmits the symmetrical fragmentation-transmission secret key to the receiving element via a ~~so-called~~ second-level relay;

-the second-level relay informs the database that the symmetrical fragmentation-transmission secret key is being used;

- the receiving element transmits to the sending element an authorization to send fragments via the second-level relay;

- the sending element fragments ~~the~~ data in ~~the~~ an initial file, according to an incremental distribution before assignment by swapping, such that the data of each fragment is unintelligible, the level and the type of fragmentation being predefined in the symmetrical fragmentation-transmission secret key;

- the sending element assigns each fragment an addressing path through a ~~so-called first-level~~ network of first-level relays;

- the sending element transmits each fragment to the receiving element via the first-level relays;

- the receiving element reassembles the fragments received, according to the instructions in the symmetrical fragmentation-transmission secret key, to recreate the initial data file;

- the receiving element sends an acknowledgement of receipt and of checking of the reassembly of the initial file to the database via the second-level relay; and

- the symmetrical fragmentation-transmission secret key is deleted from the database.

2. (Currently Amended) The method as claimed in claim 1 wherein there are defined several different classes for defining the initial ~~information object~~file to be transmitted, namely:

- a class T of fragmentation types of the bit-by-bit, byte-by-byte, byte block-by-byte block, bit block-by-bit block, space-by-space type, and therefore all possible instances for each of the abovementioned types;

- a fragmentation level class F, F being a real integer at least equal to two determined when choosing the fragmentation level;

- a network size class R, R being a real integer at least equal to one, and preferably greater than or equal to two, determined when choosing the size of the network architecture;

- a class A of IP addresses of the relays of the network architecture of the types of IP addresses of the ~~so-called~~ first-level relays, IP addresses of the ~~so-called~~ second-level relays, with all possible instances.

3. (Currently Amended) The method as claimed in claim 1, wherein the symmetrical fragmentation-transmission secret key comprises two subkeys, namely:

- a fragmentation-reassembly subkey, unique to each initial data file to be transmitted, and for which the counting possibilities are derived from the factorial

computation, comprising the instructions needed for the deletion of the initial data file and the distribution by swapping in a set of fragments;

- a sending subkey, unique to each initial data file to be transmitted, and for which the counting possibilities are derived from the exponential computation, comprising the instructions needed, such as the IP addresses of the first-level relays, for routing the fragments within the network of first-level relays.

4. (Previously Presented) The method as claimed in claim 3, wherein the receiving element addresses a request to the first-level relays, the IP address of which is contained in the sending subkey, to download the fragments.

5. (Previously Presented) The method as claimed in claim 1, wherein each of the first-level relays is provided with management means for recognizing incoming fragments, intelligent sorting and forwarding the same fragments to their recipient.

6. (Previously Presented) The method as claimed in claim 1, wherein the second-level relay is not linked to the network of first-level relays.

7. (Previously Presented) The method as claimed in claim 1, wherein the network of first-level relays is dependent on the second-level relay for the definition of readdressing tasks.

8. (Previously Presented) The method as claimed in claim 1, wherein a first-level relay or second-level relay is replaced by three in-line relays, the intermediate relay of which is an IP address linked to the other two relays via a non-Internet connection.